(56) **References Cited**

OTHER PUBLICATIONS

A list of popular password cracking wordlists. 2005. Date Accessed Sep. 2, 2014. http://www.outpost9.com/files/WordLists.html.

Mazurek et al., Measuring Password Guessability for an Entire University. Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13). 2013: 173-186.

De Luca et al., PassShape—stroke based shape passwords. Proceedings of OzCHI. 2007: 1-2.

Narayanan and Shmatikov .Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff. CCS'05. 2005: 1-9.

Vance. If your password is 123456, just make it hackme. New York Times. 2010. Date Accessed Sep. 2, 2014. http://www.nytimes.com/2010/01/21/technology/21password.html.

Bernd Chang. 6 Million User Data of China Software Developer Network (CSDN) Leaked. HUG China. 2011. Date Accessed Sep. 18, 2014. http://www.hugchina.com/china/stories/science/6-million-user-data-of-china-software-developer-network-csdn-leaked-2011-12-22.html.

Castelluccia et al., Adaptive password-strength meters from Markov models. NDSS '12. 2012.

Schweitzer et al., Visualizing keyboard pattern password. 6th International Workshop on Visualization for Cyber Security. 2009: 69-73.

Klein. Foiling the cracker: a survey of and improvements to password security. Proceedings of USENIX UNIX Security Workshop. 1990: 1-11.

Ma et al., A Study of Probabilistic Password Models. Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP '14). 2014: 1-16.

Hashcat advanced password recovery. Last updated Aug. 20, 2014. Date Accessed Sep. 18, 2014. http://hashcat.net/oclhashcat/.

Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. 2012 IEEE Symposium on Security and Privacy. 2012: 538-552.

Yan et al., Password Memorability and Security: Empirical Results. IEEE Security and Privacy Magazine. 2004. Volume 2: 25-31.

Bonneau and Shutova. Linguistic properties of multi-word passphrases. Proceedings of the 16th international conference on Financial Cryptography and Data Security. 2010: 1-12.

Bensmann. Intelligent Search Strategies on Human Chosen Passwords. Doctoral dissertation, Master's thesis. Technische Universitaet Dortmund. 2009: 1-96.

Kuo et al., Human Selection of Mnemonic Phrase-based Passwords. Symp. On Usable Privacy and Security (SOUPS). 2006: 1-12.

Rabiner. A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. Proceedings of the IEEE. 1989. Volume 77 (No. 2): 257-286.

Dell'Amico et al., Password strength: an empirical analysis. Proceedings of IEEE INFOCOM 2010. 2010: 1-9.

Hellman et al., A Cryptanalytic Time-Memory Trade-Off. IEEE Transactions on Information Theory. 1980. vol. 6 (Issue 4): 401-406.

Weir et al., Password cracking using probabilistic context-free grammars Proceedings of the 30th IEEE Symposium on Security and Privacy. 2009: 391-405.

Weir et al., Testing metrics for password creation policies by attacking large sets of revealed passwords. Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS '10). Chicago, Illinois. 2010: 162-175.

Shay et al, Can Long Passwords be secure and usable? Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14). 2014: 1-10.

Mentens et al., Time-Memory Trade-Off Attack on FPGA Platforms: UNIX Password Cracking. Proceedings of the International Workshop on Reconfigurable Computing: Architectures and Applications. Lecture Notes in Computer Science. 2006. Volume 3985: 323-334.

Kelley et al., Guess again (and again and again): measuring password strength by simulating password-cracking algorithms. Proceedings of the 2012 IEEE Symposium on Security and Privacy. 2012: 523-537.

Oechslin. Making a Faster Cryptanalytic Time-Memory Trade-Off. Proceedings of Advances in Cryptology (CRYPTO 2003). Lecture Notes in Computer Science. Volume 2729: 617-630.

McMillan. Phishing attack targets MySpace users. 2006. Date Accessed Sep. 2, 2014. http://www.infoworld.com/d/security-central/phishing-attack-targets-myspace-users-614.

Shay et al, Encountering stronger password requirements: user attitudes and behaviors. 6th Symposium on Usable Privacy and Security (SOUPS). Redmond, WA. 2010: 1-20.

Houshmand and Aggarwal. Building better passwords using probabilistic techniques. Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12). 2012: 109-118.

Musil. Hackers post 450K credentials pilfered from Yahoo. CNET. 2012. Date Accessed Sep. 18, 2014. http://www.cnet.com/news/hackers-post-450k-credentials-pilfered -from-yahoo/.

Riley. Password security: what users know and what they actually do. Usability News. 2006. vol. 8 (No. 1): 1-5.

Stone-Gross et al., Your botnet is my botnet: Analysis of a botnet takeover. Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09). Chicago, Illinois. 2009: 635-347.

Schetcher et al., Popularity is everything: a new approach to protecting passwords from statistical-guessing attacks. HotSec'10: Proceedings of the 5th USENIX conference on Hot Topics in Security. 2010: 1-6.

Warren. Thousands of Hotmail Passwords Leaked. 2009. Date Accessed Sep. 2, 2014. http://www.neowin.net/news/main/09/10/05/thousands-of-hotmail-passwords-leaked-online.

The Open wall group,.John the Ripper password cracker. Date Accessed Jul. 30, 2014. http://www.openwall.com/john/.

Zhang et al., The security of modern password expiration: an algorithmic framework and empirical analysis. Proceedings of 17th ACM Conference on Computer and Communication Security (CCS '10). Chicago, Illinois. 2010:176-186.

Wikipedia, "NTLM". Date Accessed Jun. 2, 2013. http://en.wikipedia.org/wiki/NTLM.

TrueCrypt Free Open-Source On-the-fly Encryption. Date Accessed Jun. 2, 2013. http://www.truecrypt.org/.

Manber. A simple scheme to make passwords based on one-way functions much harder to crack. Computers & Security Journal. 1996. vol. 15. (Issue 2): 171-176.

Weir. RE: Test the Strength of Your Password Creation Policy. 2009. Date Accessed Jun. 2, 2013. http://reusablesec.blogspot.com/2009/06/re-test-strength-of-your-password.html.

Weir. Probabilistic Password Cracker—Reusable Security Tools. Date Accessed Jun. 2, 2013. http://sites.google.com/site/reusablesec/Home/password-cracking-tools/probablistic_cracker.

Cain & Able Password Cracker. 2013. Date Accessed Jun. 2, 2013. http://www.oxid.it.

Chomsky. Three models for the description of language. IEEE Transactions on Information Theory. 1956. vol. 2 (No. 3): 113-124.

John the Ripper's cracking modes. Date Accessed Jun. 2, 2013. http://www.openwall.com/john/doc/MODES.shtml.

Naraine. PhpBB Hacked; Details Scarce. ZDNet. Date Accessed Jun. 2, 2013 http://blogs.zdnet.com/security/?p=2493.

Weir and Aggarwal. Cracking 400,000 Passwords or How to Explain to Your Roommate why the Power-Bill is a Little High. Defcon 17. 2009: 1-78.

Password Weir. Reusable Security: Password Cracking, Crypto, and General Security Research. Blog. 2010. Date Accessed Jun. 2, 2013. http://reusablesec.blogspot.com.

Veras et al., On the Semantic Patterns of Passwords and their Security Impact. Network and Distributed System Security Symposium (NDDS '14). 2014: 1-16.

Weir. Using Probabilistic Techniques to aid in Password Cracking Attacks. Dissertation. Florida State University. 2010: 1-140.

* cited by examiner